Bijlage:
Keuze EAL-niveau voor Common Criteria certificering

Inleiding

De Deskundigengroep heeft opdracht gekregen de specificaties op te stellen voor de stemprinter en stemmenteller, waaronder de Protection Profiles voor de Common Criteria certificering die de commissie Van Beek heeft geadviseerd.

Een van de (vele) punten van overweging met betrekking tot de Protection Profiles is het zogenaamde EAL-niveau waartegen de Common Criteria certificering moet plaatsvinden.

De commissie Van Beek heeft in haar rapport van december 2013 over het EAL-niveau het volgende geadviseerd:
"Vanwege de maatregelen die de commissie wenselijk acht gaat zij er vanuit dat minimaal EAL-niveau 5 zal moeten worden gebruikt. Mogelijk zal er voor de stemprinter een ander niveau moeten worden gebruikt dan voor de scanner (de stemmenteller)."

In deze bijlage wordt nader ingegaan op de EAL-materie en op de keuzen van de Deskundigengroep omtrent het voor de Protection Profiles te hanteren EAL-niveau.

Evaluation Assurance Level

Binnen het stelsel van de Common Criteria wordt met de Evaluation Assurance Level (EAL) aangeduid met welke diepgang de evaluatie wordt uitgevoerd op de te certificeren producten. Hoe hoger het EAL-niveau, hoe groter de diepgang waarmee is getoetst dat de implementatie van het product voldoet aan hetgeen in de Protection Profiles is bepaald ten aanzien van de beveiliging van de te certificeren objecten. Het EAL-niveau bepaalt derhalve de mate van zekerheid die men kan krijgen omtrent de vraag of de beveiligingsmaatregelen die in een Protection Profile staan zijn geïmplementeerd.

Het EAL-niveau bepaalt dus niet direct de mate van beveiliging. De mate van beveiliging wordt bepaald door de beveiligingsmaatregelen die zijn beschreven in een Protection Profile. De enige uitzondering op deze regel is de zekerheidsklasse AVA (Assurance Vulnerability Analysis), die niet alleen het niveau of de intensiteit van de kwetsbaarheidsanalyse vaststelt, maar ook het aanvalspotentieel, ofwel de moeite die een potentiële aanvaller moet doen om in te breken in het systeem. De keuze voor een hogere AVA-klasse vereist bescherming tegen een hoger aanvalspotentieel.

Een EAL-niveau correspondeert met een pakket aan zekerheidscontroles. Deze zekerheidscontroles zijn ingedeeld in klassen, daarbinnen in families en daarbinnen weer in zekerheidscomponenten:

- Een klasse geeft een eerste categorisering van de zekerheidscontroles, zoals de wijze waarop het systeem ontwikkeld en gedocumenteerd moeten worden (Development), de wijze waarop het systeem functioneel getest moet worden (Test) en de kwetsbaarheidanalyses die de evaluator moet uitvoeren (Vulnerability assessment). Een klasse wordt afgekort met drie letters, in het voorbeeld is dat "ADV", "ATE" en "AVA".
- Een familie geeft binnen een klasse een verdere indeling, bijvoorbeeld bij functionele testen van de beveiliging de dekking van de testen, de diepgang van de testen, de documentatie/ vastlegging van de testen en het uitvoeren van functionele testen door een evaluator. Een familie wordt aangeduid met de code voor de klasse plus een drieletterige code voor de familie, voor het uitvoeren van functionele testen door de evaluator is dat "ATE_IND".

- Een zekerheidscomponent is binnen een familie een pakket aan zekerheidscontroles. Dit wordt aangeduid met een cijfer en is bij een hoger nummer altijd een uitgebreider pakket, dus met meer diepgang in de evaluatie. Bijvoorbeeld in de familie functionele testen door de evaluator (ATE_IND) loopt het op van het door de evaluator functioneel testen voor een deel van de beveiliging gerelateerde functionaliteit (cijfer 1) tot het functioneel testen van alle beveiliging gerelateerde functionaliteit en tevens het herhalen van alle ook door de leverancier uitgevoerde en gedocumenteerde functionele testen (cijfer 3).

In onderstaande tabel is per klasse en daarbinnen de familie weergegeven welke zekerheidscomponent bij een EAL-niveau hoort. Ofwel wat de diepgang van de evaluatie is op het betreffende onderwerp.

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Deze tabel maakt duidelijk dat voor de meeste families een hoger EAL leidt tot een uitgebreidere evaluatie. Bij de klasse Vulnerability Assessment, bijvoorbeeld, neemt de diepgang van de kwetsbaarheidsanalyse (AVA_VAN) toe van AVA_VAN.1 bij EAL1 tot AVA_VAN.5 bij EAL7. Bij sommige families is ongeacht het EAL-niveau de diepgang in de evaluatie hetzelfde. Een voorbeeld om dit te illustreren: binnen de klasse “Guidance documents” wordt bij de “Operationele user

guidance" gecodeerd met AGD_OPE de gebruikersdocumentatie bij elk mogelijk EAL-niveau met dezelfde diepgang (zijnde 1) geëvalueerd. De tabel laat ook zien dat er één familie is die in geen enkel EAL wordt gebruikt. In de klasse Life-Cycle Support wordt voor 'Flaw remediation' (ALC_FLR), ofwel het in kaart brengen en verhelpen van potentiële beveiligingsproblemen, niet één van de mogelijke zekerheidscomponenten (ALC_FLR.1 tot en met ALC_FLR.3) gebruikt in een EAL.

Overwegingen bij de selectie van het Evaluation Assurance Level

Over het algemeen genomen leiden alle zekerheidscomponenten tot meerwaarde, maar ook tot extra kosten voor het certificeringsproces. Een CC-evaluatie duurt doorgaans zes tot twaalf maanden; dit hangt onder meer af van de betreffende zekerheidscomponenten. Voor productwijzigingen is een deltacertificering vereist, die eveneens tot extra kosten leidt per zekerheidscomponent. Het spreekt voor zich dat een langdurige certificeringsprocedure problematisch kan zijn gezien de strikte deadlines die bij verkiezingen gelden. Mede daarom is het van belang om de zekerheidscomponenten zorgvuldig te selecteren.

In de stemprinter en stemmenteller kunnen standaardcomponenten zijn verwerkt (apparatuur en programmatuur), zoals besturingssysteem, beeldschermen, printers, scanners enz. Het gebruik van dergelijke standaardcomponenten biedt voordelen (in zowel tijd als geld) bij de ontwikkeling van apparatuur, maar kan tegelijkertijd de evaluatie complexer maken. Mogelijk zijn deze zekerheidscomponenten niet volgens CC-vereisten ontwikkeld, of is ten behoeve van de evaluatie geen volledige documentatie voorhanden. Zekerheidscomponenten voor evaluatie die beperkingen opleggen aan de ontwikkeling van standaardcomponenten kunnen het gebruik daarvan lastig of zelfs onmogelijk maken. De zekerheidscomponenten moeten daarom zodanig worden gekozen dat dit risico minimaal blijft.

Het gekozen Evaluation Assurance Model

Voor de Protection Profiles voor de stemprinter en stemmenteller is gekozen voor EAL4, en wel om de volgende redenen:

- EAL4 omvat een code review, maar de lagere niveaus niet. Een code review kan het vertrouwen (van het publiek) vergroten en kan potentiële beveiligingskwetsbaarheden aan het licht brengen;
- EAL5 en hoger voegen zekerheidscomponenten toe die het gebruik van standaardcomponenten (apparatuur en programmatuur) ernstig bemoeilijken maar niet per se bijdragen aan de beveiliging van het product;
- Zekerheidscomponenten waarvan de extra beveiligingswaarde opweegt tegen de kosten kunnen als "extra's" aan EAL4 worden toegevoegd (EAL4+).

Overzicht van relevante zekerheidscomponenten

Wanneer EAL4 wordt gekozen voor de Protection Profiles kan voor bepaalde aspecten in een CC-certificering toch het zekerheidsniveau van hogere EAL's worden bereikt. Daartoe dient voor elke zekerheidscomponent die nog niet bij EAL4 is ondergebracht te worden vastgesteld of die component in het Protection Profile aan EAL4 moet worden toegevoegd. Deze "plussen" in aanvulling op EAL4 worden "augmentations" genoemd. De onderstaande tabel geeft de standaard zekerheidscomponenten weer die wel in de CC zijn gespecificeerd, maar geen deel uitmaken van EAL4. Dit zijn dus de zekerheidscomponenten die eventueel als augmentations toegevoegd kunnen worden aan de Protection Profiles voor de stemprinter en stemmenteller. In de tabel wordt ook beargumenteerd waarom de zekerheidscomponent wel of niet zou moeten worden opgenomen als augmentation in aanvulling op EAL4 in de Protection Profiles. Het criterium daarvoor is dat een

zekerheidscomponent moet bijdragen aan de beveiliging van de stemprinter en stemmenteller en het gebruik van standaardcomponenten (programmatuur en apparatuur) niet geheel mag uitsluiten.

De tabel is als volgt opgebouwd:

- Kolom 1: bevat de codes van de zekerheidscomponenten die niet “standaard” tot EAL4 behoren. Die zekerheidscomponenten kunnen in de vorm van een augmentation aan EAL4 worden toegevoegd. Als een zekerheidscomponent tot een hogere EAL-klasse behoort, is in deze kolom weergegeven bij welke EAL-niveaus die zekerheidscomponent wel is inbegrepen.
- Kolom 2: geeft inhoudelijk weer wat de betreffende zekerheidscomponent inhoudt.
- Kolom 3: argumenten ter overweging om een zekerheidscomponent al dan niet op te nemen.

<table>
<tr><th>Zekerheids component (zit in EAL)</th><th>Omvat</th><th>Argumenten voor of tegen opname van een augmentation als aanvulling op EAL4</th></tr>
<tr><td>ADV</td><td colspan="2">Ontwikkeling</td></tr>
<tr><td>ADV_FSP.5
(EAL 5,6)</td><td>De functionele specificatie van beveiligingsgerelateerde functies moet op een semi-formele wijze worden opgesteld (zoals Unified Modeling Language).</td><td rowspan="2">De augmentation ADV_FSP.5 leidt tot aanvullende eisen omdat daardoor een semi-formele aanpak en het verschaffen van uitgebreide fouteninfo verplicht is.
Dit bevordert de controleerbaarheid en transparantie doordat het de functionele specificatie van de beveiligings gerelateerde functies eenduidig maakt en de analyse van foutcondities ondersteunt.
Een gestructureerde, semi-formele benadering wordt veel gebruikt voor functionele specificaties. De grondige aandacht voor foutcondities draagt bij aan de kwaliteitsborging van het product.
Deze augmentation maakt het gebruik van standaardcomponenten mogelijk lastiger als de beveiligingsgerelateerde functies daarvan nog niet semi-formeel zijn beschreven, maar niet onmogelijk.

De augmentation ADV_FSP.6 vereist een formele beschrijving van het voor de beveiliging relevante gedeelte van de productinterface en een volledige beschrijving van alle foutsituaties die kunnen optreden.
De formele beschrijving van de interface van de beveiligingsfunctionaliteit bevordert de controleerbaarheid en de transparantie.
Formele modelleringstechnieken zijn niet gangbaar in de ontwikkeling van de omvangrijkere standaard programmatuur componenten.
Deze augmentation zal het dan ook moeilijk of zelfs onmogelijk maken om standaardcomponenten te gebruiken.</td></tr>
<tr><td>ADV_FSP.6
(EAL 7)</td><td>De functionele specificatie van de beveiligingsgerelateerde functies moet op een formele wijze worden opgesteld (een wiskundige basis hebben).</td></tr>
<tr><td>ADV_IMP.2
(EAL 6,7)</td><td>Er moet een relatie gelegd worden tussen ontwerpdocumentatie van de beveiligingsgerelateerde functies en de volledige implementatie (zowel de</td><td>De augmentation ADV_IMP.2 leidt tot aanvullende eisen door verplicht te stellen dat de ontwikkelaar een volledige beschrijving van de beveiligingsgerelateerde functies verstrekt aan de evaluator, inclusief de desbetreffende ontwerpdocumentatie.</td></tr>
</table>

Zekerheids component (zit in EAL)	Omvat	Argumenten voor of tegen opname van een augmentation als aanvulling op EAL4
	programmatuur als de apparatuur).	Dit vergroot de reikwijdte van de analyse van de implementatie door de evaluator en geeft meer zekerheid omtrent de ontwikkeling. De transparantie en controleerbaarheid zijn echter al geborgd onder zekerheidscomponent ADV_IMP.1, waarbij de evaluator een specifiek onderdeel van de implementatie analyseert. Deze augmentation is bij de ontwikkeling van standaardcomponenten mogelijk niet gevolgd. Het expliciet voorschrijven dat er een relatie wordt gelegd tussen ontwerpdocumentatie en implementatie, kan dan echter leiden tot aanzienlijk zwaardere inspanningen aan de kant van de ontwikkelaar. Deze augmentation zal het dan ook moeilijker maken om standaardcomponenten te gebruiken.
ADV_INT.1	De interne opbouw van het product moet voor een deel van de beveiliginggerelateerde functies goed gestructureerd zijn.	Augmentations ADV_INT.1 en ADV_INT.2 houden een controle in dat de implementatie van (een deel van) de beveiligingsgerelateerde functies goed gestructureerd is. Een goed gestructureerde code bevordert de controleerbaarheid van het product. Door producten die heden ten dage zijn ontwikkeld zal aan dit vereiste worden voldaan. Deze augmentation staat het gebruik van standaardcomponenten derhalve niet in de weg. De augmentation ADV_INT.3 vereist daarnaast dat de opbouw van beveiligingsgerelateerde functies niet onnodig complex is. Deze augmentation bevordert weliswaar de transparantie en controleerbaarheid van het product, maar de gebruikelijke ontwikkeling van componenten is niet noodzakelijkerwijs gericht op minimalisering van de complexiteit. Dat komt doordat ontwikkelaars hun code lang niet altijd toespitsen op een specifiek gebruiksscenario, en complexe structuren handhaven die bijvoorbeeld zijn afgeschreven, maar wel bruikbaar blijven voor het onderhoud van oudere productversies. Deze augmentation kan het gebruik van standaardcomponenten dus moeilijker maken, of zelfs onmogelijk.
ADV_INT.2 (EAL 5)	De interne opbouw van de beveiligingsgerelateerde functies moet goed gestructureerd zijn.	
ADV_INT.3 (EAL 6,7)	De interne opbouw van de beveiligingsgerelateerde functies moet goed gestructureerd zijn en niet onnodig complex.	
ADV_SPM.1 (EAL 6,7)	Het beveiligingsbeleid voor specifieke beveiligingsmaatregelen van het systeem moet zijn ondergebracht in een formeel model, waarvan is bewezen dat het effectief is.	De augmentation ADV_SPM.1 stelt het op formele wijze uitwerken van beveiligingsmaatregelen verplicht. Dit vergroot de controleerbaarheid van de implementatie, aangezien onderdelen van de beveiligingsfunctionaliteit een grondig ontwerpproces moeten doorlopen. Formele modelleringstechnieken worden echter niet algemeen gebruikt bij de gebruikelijke wijze van

Zekerheids component (zit in EAL)	Omvat	Argumenten voor of tegen opname van een augmentation als aanvulling op EAL4
		ontwikkeling van programmatuur en zijn voor omvangrijke systemen mogelijk überhaupt niet toepasbaar. Deze augmentation kan het gebruik van standaardcomponenten dus moeilijker maken, of zelfs onmogelijk.
ADV_TDS.4 (EAL 5)	Het ontwerp van de beveiligingsgerelateerde deelsystemen moet semi-formeel worden opgesteld.	De augmentation ADV_TDS.4 vereist dat de ontwikkelaar semi-formele methoden hanteert voor het ontwerp van deelsystemen. Een semi-formele aanpak vermindert de ambiguïteit en vergroot de inzichtelijkheid van het ontwerp van programmatuur. Dit draagt dus bij aan de controleerbaarheid en transparantie. Semi-formele methoden voor ten minste een deel van het ontwerp worden in de ontwikkeling van programmatuur incidenteel gehanteerd, maar zijn wel de standaard praktijk bij de ontwikkeling van apparatuur. Deze augmentation zal het gebruik van standaardcomponenten lastiger maken, maar niet onmogelijk. De augmentation ADV_TDS.5 stelt het gebruik van semi-formele methoden ook op moduleniveau verplicht. In algemene zin gelden ook hier de opmerkingen ten aanzien van ADV_TDS.4, maar het zal lastiger zijn om standaard (programmatuur en apparatuur) componenten te gebruiken, omdat ontwikkelaars niet altijd semi-formele methoden tot op moduleniveau toepassen. De augmentation ADV_TDS.6 vereist het gebruik van een formeel model voor het ontwerp van beveiligingsgerelateerde deelsystemen, alsmede formeel bewijs dat het formele model overeenstemt met de functionele specificatie. Deze augmentation bevordert de controleerbaarheid van het ontwerp omdat het ontwerp een grondig ontwerpproces moeten doorlopen. Formele methoden worden bij de gebruikelijke ontwikkeling van programmatuur echter niet algemeen gebruikt en zijn voor omvangrijke systemen wellicht zelfs onmogelijk. Deze augmentation kan het gebruik van standaardcomponenten derhalve bijzonder moeilijk maken, of zelfs onmogelijk.
ADV_TDS.5 (EAL 6)	Het ontwerp van de beveiligingsgerelateerde deelsystemen moet semi-formeel worden opgesteld. Het ontwerp van de beveiligingsgerelateerde modules moet semi-formeel worden opgesteld.	
ADV_TDS.6 (EAL 7)	Het ontwerp van beveiligingsgerelateerde deelsystemen moet op een formele wijze worden opgesteld. Het ontwerp van de beveiligingsgerelateerde modules moet semi-formeel worden opgesteld. De overeenstemming met de functionele specificatie van de beveiligingsgerelateerde functies moet formeel worden bewezen.	
ALC	**Product levenscyclus**	
ALC_CMC.5 (EAL 6,7)	Wijzigingen aan het product en de (ontwerp)documentatie daarvan moeten in een geautomatiseerd	De augmentation ALC_CMC.5 vereist strikte toepassing van het configuratiemanagementsysteem en leidt tot een sterke verbetering van de registratie- en controlemogelijkheden

Zekerheids component (zit in EAL)	Omvat	Argumenten voor of tegen opname van een augmentation als aanvulling op EAL4
	configuratiemanagementsysteem worden vastgelegd. Het configuratiemanagementsysteem moet tevens aangeven dat als er ergens in het product of de documentatie iets wordt gewijzigd welke andere delen van het product of documentatie daardoor worden geraakt.	van het systeem. De kans op niet-gecontroleerde wijzigingen van een product wordt hiermee nog verder verminderd dan onder de vereisten van ALC_CMC.4, en dat komt de transparantie en controleerbaarheid ten goede. Deze augmentation is bij de ontwikkeling van standaardcomponenten echter mogelijk niet gevolgd en is dan niet of lastig achteraf alsnog toe te passen.
ALC_CMS.5 (EAL 5,6,7)	Het configuratiemanagement moet ook de gebruikte ontwikkelhulpmiddelen en daaraan gerelateerde informatie omvatten.	De augmentation ALC_CMC.5 vereist dat het configuratiemanagementsysteem ook ontwikkelhulpmiddelen omvat. Dit bevordert de controleerbaarheid en transparantie, omdat op deze manier de gehele ontwikkelomgeving nauwkeurig wordt beschreven en herstelbaar is. Als deze werkwijze nog niet wordt gehanteerd maakt deze augmentation het echter moeilijk, zo niet onmogelijk, om standaardcomponenten te gebruiken.
ALC_DVS.2 (EAL 6,7)	Uit beveiligingsdocumentatie moet blijken dat de beveiligingsmaatregelen voor het ontwerpen en ontwikkelen van het product afdoende bescherming bieden waardoor de vertrouwelijkheid en integriteit van het product is gewaarborgd.	De augmentation ALC-DVS.2 vereist dat wordt onderzocht of de beveiligingsmaatregelen voor het ontwikkelen van het product toereikend zijn. Dit bevordert de controleerbaarheid en transparantie van de beveiligingsmaatregelen. Deze verbeterde controleerbaarheid is doorgaans haalbaar indien er al beveiligingsmaatregelen voor de ontwikkeling gelden conform ALC_DVS.1. Deze augmentation vindt steeds vaker toepassing. Hij wordt bijvoorbeeld ook toegepast in het PP van de Europese Unie die geldt voor de chip in de paspoorten.
ALC_FLR.1	Er moeten processen zijn ingeregeld om aangetroffen potentiële beveiligingsgerelateerde problemen te identificeren, te analyseren en op te lossen.	Deze augmentations bevorderen de controleerbaarheid en transparantie en dragen er toe bij dat er systematische aandacht is voor de afwikkeling van potentiële beveiligings-gerelateerde problemen en het oplossen ervan. Worden deze processen nog niet uitgevoerd, dan kan dat alsnog worden gedaan na de productontwikkeling. Deze augmentations sluiten het gebruik van standaardcomponenten dus niet uit.
ALC_FLR.2	Er moeten processen zijn ingeregeld om aangetroffen potentiële beveiligingsgerelateerde problemen te identificeren, te analyseren en op te lossen. Alle gemelde potentiële beveiliginggerelateerde problemen moeten worden aangepakt.	
ALC_FLR.3	Er moeten processen zijn ingeregeld om aangetroffen potentiële	

Zekerheids component (zit in EAL)	Omvat	Argumenten voor of tegen opname van een augmentation als aanvulling op EAL4
	beveiligingsgerelateerde problemen te identificeren, te analyseren en op te lossen. Alle gemelde potentiële beveiliginggerelateerde problemen moeten worden aangepakt. Gebruikers worden tijdig op de hoogte gebracht van potentiële beveiliginggerelateerde problemen en de afwikkeling daarvan.	
ALC_LCD.2 (EAL 7)	Voor de ontwikkeling en onderhoud wordt gebruik gemaakt van metrieken om de kwaliteit van het product objectief vast te stellen, zoals metrieken voor de complexiteit van code en mean time to failure.	Deze augmentation bevordert de controleerbaarheid en transparantie doordat de kwaliteitseigenschappen van het product objectief wordt afgedwongen. Deze augmentation is voor standaardcomponenten echter mogelijk niet gevolgd en is dan niet of lastig achteraf alsnog toe te passen.
ALC_TAT.2 (EAL 5)	De toegepaste ontwikkelstandaarden moeten zijn beschreven.	De augmentations bevorderen de controleerbaarheid en transparantie. ALC_TAT.3 is voor standaardcomponenten echter mogelijk niet gevolgd en is dan niet of lastig achteraf alsnog toe te passen.
ALC_TAT.3 (EAL 6,7)	De toegepaste ontwikkelstandaarden moeten zijn beschreven, ook voor de gebruikte (standaard)producten van derden.	
ASE	**Evaluatie**	
ASE_TSS.2	Er moet voor het product een samenvatting van de specificatie van de beveiliging gerelateerde functies zijn waarin wordt beschreven hoe aan de beveiligingsdoelstellingen wordt voldaan. De samenvatting van de specificatie moet ook beschrijven hoe het product zichzelf beschermt tegen negatieve invloeden van buitenaf, manipulatie en het omzeilen van de beveiliging.	De augmentation ASE_TSS.2 vereist dat de samenvatting van de specificaties van de beveiliging gerelateerde functies wordt aangevuld met een beschrijving van het ontwerp van de beveiligingsarchitectuur van het product. De augmentation draagt bij aan de controleerbaarheid en transparantie.
ATE	**Testen**	
ATE_COV.3 (EAL 6,7)	Alle beveiliginggerelateerde functionaliteit moet aantoonbaar volledig zijn getest.	Deze augmentation zorgt ervoor dat er zo uitputtend mogelijk wordt getest. Dit bevordert de controleerbaarheid en transparantie. Deze augmentation is bij de ontwikkeling van standaardcomponenten echter mogelijk niet gevolgd en is dan niet of lastig achteraf alsnog toe te passen. Let op: dit dekt alleen het testen van de

Zekerheids component (zit in EAL)	Omvat	Argumenten voor of tegen opname van een augmentation als aanvulling op EAL4
		beveiligingsgerelateerde functionaliteit en dus niet ALLE functionaliteit.
ATE_DPT.2	De testen moeten de goede werking van alle modules die een beveiligingsmaatregel implementeren omvatten (in plaats van alleen subsystemen die een beveiligingsmaatregel implementeren).	Deze augmentations zorgen ervoor dat de beveiliging zo uitputtend mogelijk wordt getest. De augmentations ATE-DPT.2 en ATE_DTP.3 vereisen dat de beveiligingsgerelateerde modules worden getest. Deze augmentations dragen bij aan de controleerbaarheid en transparantie. Deze augmentations zijn voor standaardcomponenten echter mogelijk niet gevolgd en is dan niet of lastig achteraf alsnog toe te passen. Onder ATE_DPT.4 wordt een zeer strikte implementatietest verplicht gesteld. Dit bevordert de controleerbaarheid, maar maakt het als deze test nog niet is uitgevoerd moeilijk of zelfs onmogelijk om standaardcomponenten te gebruiken. Lagere ATE_DPT augmentations worden vaak toegepast, zoals in het PP van de Europese Unie die geldt voor de chip in de paspoorten en het PP van de Europese Unie die geldt voor de digitale tachograaf.
ATE_DPT.3 (EAL 5,6)	De testen moeten de goede werking van alle beveiligingsgerelateerde modules omvatten.	
ATE_DPT.4 (EAL 7)	De testen van de beveiligingsgerelateerde functionaliteit moeten de goede werking van alle aspecten van de implementatie (in zowel de programmatuur als de apparatuur) omvatten.	
ATE_FUN.2 (EAL 6,7)	Bij het testen moet ook meegenomen zijn of de volgorde van testen invloed kan hebben op de uitkomst en daardoor fouten verborgen zouden kunnen blijven.	Deze augmentation zorgt ervoor dat de beveiliging zo uitputtend mogelijk wordt getest. De augmentation draagt bij aan de controleerbaarheid en transparantie.
ATE_IND.3 (EAL 7)	De evaluator herhaalt alle door de ontwikkelaar uitgevoerde testen van de beveiligingsgerelateerde functionaliteit in plaats van maar een deel om de uitkomsten van die testen te valideren. De evaluator test zelf ook alle beveiligingsgerelateerde functionaliteit in plaats van alleen een deel daarvan.	De augmentation ATE_IND.3 vereist dat de evaluator alle beveiligingsgerelateerde tests herhaalt. Deze augmentation verbreedt weliswaar de dekking van de verificatie, maar leidt niet tot meer controleerbaarheid en transparantie omdat hetgeen wordt getest (zoals gedefinieerd in ATE_FUN en ATE_DPT) niet toeneemt.
AVA	**Kwetsbaarheidsanalyse**	
AVA_VAN.4 (EAL 5)	De evaluator moet de kwetsbaarheidsanalyse methodisch uitvoeren. De evaluator voert penetratietesten uit op basis van een aanvaller met een **matig aanvalsniveau**.	De augmentations AVA_VAN.4 en AVA_VAN.5 vereisen een methodische benadering van de kwetsbaarheidsanalyse en geven ook een definitie van het veronderstelde aanvalsniveau. De keuze van het aanvalsniveau is afhankelijk van de waarde van hetgeen beschermd moet worden en de moeite die een aanvaller zich naar verwachting zou willen getroosten. Een methodische benadering van de kwetsbaarheidsanalyse waarborgt dat de beveiliging van het product zo uitputtend
AVA_VAN.5 (EAL 6,7)	De evaluator moet de kwetsbaarheidsanalyse methodisch uitvoeren. De	

Zekerheids component (zit in EAL)	Omvat	Argumenten voor of tegen opname van een augmentation als aanvulling op EAL4
	evaluator voert penetratietesten uit op basis van een aanvaller met een **hoog aanvalsniveau**.	mogelijk wordt geëvalueerd. Het aanvalsniveau verwijst naar de soorten aanvallen waar rekening mee wordt gehouden. Dit vereist op zijn beurt een meer defensieve en robuuste productimplementatie. Deze augmentation waarborgt dat de beveiliging wordt gecontroleerd. Deze augmentation wordt veel toegepast als aanvulling op EAL4. Vaak wordt voor hoogwaardige bescherming het hoogste aanvalsniveau gekozen. AVA_VAN.5 wordt bijvoorbeeld ook toegepast in het PP van de Europese Unie die geldt voor de chip in de paspoorten en het PP van de Europese Unie die geldt voor de digitale tachograaf. Afhankelijk van de beveiligingsvereisten voor de afzonderlijke onderdelen van het systeem kan het gebruik van “kant-en-klare” standaardcomponenten lastig zijn als bij de ontwikkeling daarvan de beveiliging geen rol heeft gespeeld. Als een standaardcomponent echter niet bestand is tegen het veronderstelde hoge aanvalsniveau, dan is hij niet geschikt voor het beoogde doel. Verder hoeven niet alle standaardcomponenten in het systeem in gelijke mate bij te dragen aan de beveiliging van dat systeem. Als er bijvoorbeeld een sterk beveiligde component aanwezig is die actief fysieke inbraakpogingen detecteert, kunnen daarnaast ook standaardcomponenten worden gebruikt die slechts tegen misbruik van functionaliteit bestand zijn.

Selectie van zekerheidscomponenten

Geheel op maat gemaakte apparatuur waarin geen enkele standaardcomponent (programmatuur en apparatuur) wordt gebruikt, zal leiden tot een zeer complex en daarom extra risicovol ontwerp- en ontwikkelingstraject van de stemprinter en stemmenteller. De Deskundigengroep kiest daarom niet voor zekerheidscomponenten die het gebruik van standaardcomponenten uitsluiten.

De Deskundigengroep kiest wel voor het in de Protection Profiles opnemen van AVA_VAN.5. Deze zekerheidscomponent betreft een penetratietest en is bedoeld om zekerheid te verschaffen dat stemprinter/stemmenteller bestand is tegen geavanceerde aanvallen. Een penetratietest heeft betrekking op tal van bedreigingen in verband met fysieke en logische beveiliging, zoals ongeautoriseerd vervangen van verkiezingsgegevens en programmatuur, manipulatie van elektronica door externe krachten (bv. magnetische of elektrische pulsen) en onbedoeld uitlekken van informatie (bv. via straling of licht). Bijvoorbeeld het via elektromagnetische straling uitlekken van de stemkeuze van een kiezer, wat het geval was bij de stemmachines die tot en met 2007 zijn gebruikt, zou in een dergelijke test opgemerkt moeten worden.

Verder kiest de Deskundigengroep voor het in de Protection Profiles opnemen van ALC_DVS.2. Deze zekerheidscomponent versterkt het vertrouwen dat de stemprinter/stemmenteller op veilige wijze zijn ontwikkeld en vermindert het risico van manipulatie tijdens het ontwikkelingsproces.

Van verscheidene andere zekerheidscomponenten (ADV_FSP.5, ADV_IMP.2, ADV_INT.2, ADV_TDS.5, ALC_FLR.3, ALC_TAT.3, ASE_TSS.2, ATE_COV.3, ATE_DPT.3, ATE_FUN.2 en ATE_IND.3) die het gebruik van standaardcomponenten (programmatuur en apparatuur) niet uitsluiten, zou naar de mening van de Deskundigengroep de toegevoegde waarde niet opwegen tegen de extra complexiteit en doorlooptijd van de evaluatie die deze zekerheidscomponenten met zich meebrengen. Daarom heeft de Deskundigengroep deze zekerheidscomponenten niet in de Protection Profiles opgenomen.

Maatwerk-zekerheidscomponent in aanvulling op EAL4

Naast de standaard zekerheidscomponenten is er ook een maatwerk-zekerheidscomponent toegevoegd, te weten ALC_DEL.2. De achtergrond hiervan is dat een CC-evaluatie is gebaseerd op de controle van slechts enkele stemprinters en stemmentellers. Bij de massaproductie van stemprinters en stemmentellers kunnen afwijkingen van de geëvalueerde exemplaren voorkomen die bedoelde of onbedoelde gevolgen hebben voor de beveiliging. De zekerheidscomponent ALC_DEL.2 schrijft voor dat gecontroleerd wordt dat elke geproduceerde stemprinter en stemmenteller identiek is aan de geëvalueerde exemplaren van de stemprinter en stemmenteller. Een onafhankelijke deskundige dient te verifiëren en officieel te bevestigen dat elke geproduceerde stemprinter en stemmenteller identiek is aan de geëvalueerde exemplaren van de stemprinter en stemmenteller.

Conclusie

Het gekozen EAL is EAL4+, aangevuld met ALC_DVS.2, AVA_VAN.5 en maatwerk-zekerheidscomponent ALC_DEL.2.

- EAL4+: Dit is het hoogste EAL waarbij nog standaardcomponenten gebruikt kunnen worden. Dit niveau omvat een broncode analyse die bij kan dragen aan het vertrouwen en potentiële beveiligingsproblemen in beeld kan brengen bij de evaluatie.
- AVA_VAN.5: Voert een penetratietest uit om aan te tonen dat het systeem goed bestand is tegen een aanvaller met een hoog aanvalspotentieel. Deze zekerheidscomponent biedt het vertrouwen dat de oplossing bestand is tegen een hoog aanvalspotentieel.

- ALC_DVS.2: Aangetoond moet worden dat de beveiligingsmaatregelen toereikend zijn.
  Deze zekerheidscomponent biedt een extra waarborg dat er in de ontwikkelings- en productieomgeving rekening wordt gehouden met beveiligingsvereisten.
- ALC_DEL.2: Schrijft voor dat door een onafhankelijke deskundige wordt gecontroleerd dat elke geproduceerde stemprinter/stemmenteller identiek is aan de geëvalueerde exemplaren.